REMARKS

Claims 1-12 and 14-26 are pending in the application. Claims 1, 6, 8, 15, 17, and 20 have been amended. No new matter has been added. Applicant reserves the right to pursue the original claims and other claims in this and other applications.

Applicant appreciates the time and attention of the Patent Examiners during an Interview with Applicant's representative on April 10, 2007, where the cited art and the claimed invention were discussed. During the Interview, Applicant's representative highlighted the differences between the claimed invention and the cited art.

Claims 1, 6-8, 14-20 and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Serceki et al. (U.S. Pat. Pub. No. 20030078072)("Serceki") in view Lewis (U.S. Pat. No. 6,453,159)("Lewis"). This rejection is respectfully traversed.

Claim 1 recites a method of updating and using an encryption key used by a wireless station for encrypted communications with a wired portion of the network, said method comprising: "physically separating from said wireless station a network communications device; physically connecting said separated network communications device to an encryption key updating device which is connected to a wired portion of said network said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device; replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network; physically reconnecting said network communications device containing said new encryption key with said wireless station of said network; and accessing said encryption key on said network communications device during an encrypted communication."

Serceki discloses a "method for providing configuration information for use in installing a new wireless station to a wireless network that minimizes errors..." According to Serceki, the "configuration information is distributed by storing the configuration information onto a device with a memory and then distributing the device to the users interested in installing new wireless stations. The device is attached to a computer to which the wireless station is coupled, initiating a transfer of the configuration information. The computer uses the

configuration information to configure the wireless station. The method also provides a way to limit access to the configuration information through the use of encryption and limiting the number of times the configuration information is retrieved. The method is also an effective way to distribute security keys for encryption systems whose purpose is to secure communications in a wireless network." (Serceki, Abstract)

As articulated in the Office Action dated October 6, 2006, Serceki fails to disclose "accessing said encryption key on said network communication device during an encrypted communication." (emphasis added). The invention of Serceki is essentially a method of transferring information between two computers systems that are not physically connected by using a storage device as a conduit between the two systems, e.g., a "wireless station" and a "wired portion of a network." Thus, in the invention of Serceki, a storage device is used to transfer data, e.g., configuration information or security keys, between the two systems. As such, the invention of Serceki is different from the claimed invention and the rejection of this claim should be withdrawn for at least the reason noted.

Lewis discloses a "multi-level encryption scheme ... for a wireless network. A first level of encryption is provided primarily for wireless communications taking place between a mobile terminal and an access point. In addition, a second, higher level of encryption is provided which is distributed beyond the wireless communications onto the system backbone itself. Through a key distribution server/access point arrangement, the second level of encryption provides a secure means for distributing the encryption scheme of the first level without compromising the integrity of the network." (Lewis, Abstract)

Lewis also fails to disclose "accessing said encryption key on said network communications device during an encrypted communication." Lewis is essentially a method of decrypting an encryption key using a master key. "The mobile terminal 66 continues to provide the MASTER key to the encryption engine 94 via line 96. Thus, when the encrypted response packet containing the ENCRYPT key is received by the mobile terminal 66 it will be successfully decrypted using the MASTER key as represented by step 208." (Lewis, col. 12, lines 31-36) Thus, according to Lewis, a master key is used by a mobile terminal to decrypt an encryption key. As such, the invention of Lewis is different from the claimed invention and does

not cure the deficiencies of Serceki. The rejection of this claim should be withdrawn for at least the reasons noted above.

As such, the rejection of claim 1 should be withdrawn and the claim allowed over Serceki separately and in combination with Lewis.

Claims 6-7 depend from claim 1 and are allowable for at least the reasons noted above with respect to claim 1.

Claims 8, 14-20, and 26 have similar limitations as claim 1 and are allowable for at least the reasons noted above with respect to claim 1. Accordingly the rejection of those claims should be withdrawn and the claims allowed over Serceki and/or Lewis.

Claims 2-3, 9-10, and 21-23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Serceki in view Campbell, Jr. (U.S. Pat. No. 4,369,332)("Campbell"). This rejection is respectfully traversed.

Claims 2-3, 9-10, and 21-23 have similar limitations as claim 1 and are allowable over Serceki for at least the reasons noted above with respect to claim 1.

Campbell discloses an "apparatus and method for generating a unique working key variable for controlling the operation of an encryption/decryption device during each user specified time period. The apparatus generates each working key variable by encrypting a user specified value, unique for each specified time period, under control of a fixed key variable stored in the apparatus. After the user specified value has been encrypted, the apparatus utilizes the encrypted (working) key variable to control the encryption/decryption of data during the corresponding user specified time period." (Campbell, Abstract)

Campbell fails to disclose "accessing said encryption key on said network communications device during an encrypted communication." As such, Campbell fails to cure the deficiencies of Serceki. Therefore the rejection of these claims should be withdrawn and the claims allowed.

Claims 4-5, 11-12 and 24-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Serceki et al. (U.S. Pat. Pub. No. 20030078072)("Serceki") in view Trieger (U.S. Pat. No. 6,226,750)("Trieger"). This rejection is respectfully traversed.

Claims 4-5, 11-12 and 24-25 have similar limitations as claim 1 and are allowable over Serceki for at least the reasons noted above with respect to claim 1.

Trieger disclose a "method and system for tracking communications in a client-server environment. The method includes the steps of sending a first request from the client to the server over a first connection, sending a first key from the server to the client over the first connection, sending the first key from the client and a second request to the server over a second connection, and sending a response to the second request and a second key distinct from the first key from the server to the client over the second connection. The system includes a client for establishing a terminal connection with a server and a server in communication with the client. The server further includes key generator means generating a plurality of keys for transmission to the client, authentication means in communication with the key generator means receiving the keys from the client to recognize the keys at the server, and discarding means linked to the key generator means for disposing of previously transmitted keys." (Trieger, Abstract)

Like Serceki, Trieger also fails to disclose "accessing said encryption key on said network communications device during an encrypted communication." As such, Trieger fails to cure the deficiencies of Serceki. Therefore the rejection of these claims should be withdrawn and the claims allowed.

In view of the above amendment, Applicant believes the pending application is in condition for allowance.

Dated: April 17, 2007

Respectfully submitted,

By #41,198

Thomas J. D'Amico
Registration No.: 28,371
Michael A. Weinstein
Registration No. 53,754
DICKSTEIN SHAPIRO LLP
1825 Eye Street, NW
Washington, DC 20006-5403
(202) 420-2200
Attorney for Applicant